Machine Translated by Google

TECHDISPATCH

# CENTRALBANKEN DIGITAL VALUTA

EDPS

Machine Translated by Google

EDPS TechDispatch

HTML ISBN 978-92-9242-714-6 ISSN-nummer 2599-932X doi: 10.2804/382187 QT-AD-23-001-DA-Q

PDF-fil ISBN 978-92-9242-711-5 ISSN-nummer 2599-932X doi: 10.2804/109194 QT-AD-23-001-DA-N

Machine Translated by Google



# Centralbanken digital valuta

Lande verden over undersøger, om de skal tilbyde centralbankpenge til offentligheden ikke kun som pengesedler og mønter, men også i digital form. Det faktum, at størstedelen af centralbanker verden over allerede er begyndt at undersøge muligheden for at lancere en statsejet digital valuta som en reaktion på den øgede anvendelse af digitale, kontaktløse betalinger, kryptovalutaer og e-handel, yderligere accelereret af Covid-19, og også på grund af de muligheder, som disse digitale valutaer tilbyder som et mere fleksibelt monetært værktøj sammenlignet med den eksisterende ikke-digitale valuta. Privatliv, beskyttelse af personoplysninger og sikkerhed er blandt de vigtigste krav, som påvirker de centrale designvalg, der skal træffes, samt forventet borgernes tillid og accept.

Machine Translated by Google



# 1. Hvad er en centralbank digital valuta?

Penge kan primært eksistere i to former[1]: centralbankpenge og private penge.

Penge skabt af centralbanker er centralbankpenge, og kontanter er i øjeblikket den eneste form for centralbankpenge, der er tilgængelig for offentligheden. Faktisk er kontanter en fysisk token i form af mønter og pengesedler, der repræsenterer værdi. Blot at holde tokenet betyder, at man lovligt besidder det. Overførsler kan udføres ved at udveksle det mellem to personer uden behov for en tredjepart (som en bank) til at validere transaktionen. Kontanter **skal accepteres, hvis de tilbydes som betaling inden for en jurisdiktion** (begreb, der definerer "lovligt betalingsmiddel"[2]).

Private penge skabes af kommercielle banker, når de modtager[3] kontanter i indskud og genbruger dem ved at yde lån. Disse penge vises på bankkontoen, og de kan bruges til at betale med forskellige instrumenter såsom debet- eller kreditkort. Penge kan derefter hæves i form af kontanter, tilbage til deres oprindelige form af centralbankpenge. Forholdet mellem indehavere og kommercielle banker er baseret på tilliden til, at pengene opbevares sikkert og med acceptable risici. I dag findes der intet betalingsinstrument udover kontanter, der har status som lovligt betalingsmiddel.

En centralbanks digital valuta (CBDC) er en **digital form for offentlige penge udstedt af en centralbank.** Et CBDC-system består i bund og grund af enkeltpersoner og virksomheder, der har adgang til en digital valuta, som stilles til rådighed for dem til transaktioner og opsparingskonti af deres hjemlands centralbank. Der kan skelnes mellem detail-CBDC, der er tilgængelig for borgere og virksomheder, og engros-CBDC, der kun er tilgængelig for finansielle aktører. I denne TechDispatch vil vi primært henvise til detail-CBDC.

Med andre ord består CBDC af en digital repræsentation af mønter og pengesedler i form af digitale tokens. Det er en elektronisk fil, der indeholder en specifik værdi **med en reference til dens ejer** knyttet til den. Ved blot at ændre denne reference overføres værdien, og en betaling foretages. CBDC præsenteres normalt af centralbanker som et supplement til kontanter, udstyret med lignende funktioner (især under hensyntagen til status som lovligt betalingsmiddel), men tilpasset nogle funktionelle behov og den 'digitale' karakter, der er nævnt ovenfor.

1. For mere information om penge, valuta og værdi, se Den Europæiske Centralbank, Hvad er penge?, 2017 - **https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.da.html**
2. Status som "lovligt betalingsmiddel" er en central egenskab ved valuta: den giver en debitor ret til at opfylde monetære forpligtelser ved at tilbyde valuta til kreditoren – Den Internationale Valutafond, Juridiske aspekter af centralbankens digitale valuta: Centralbank- og pengeretlige overvejelser, WP/20/254, side 8.
3. Herefter også benævnt private banker og finansielle formidlere. For yderligere information, se venligst Investopedia, How Banking Works, Types of Banks, and How To Choose the Best Bank for You, tilgået i november 2022 - **https://www.investopedia.com/terms/b/bank.asp**

Machine Translated by Google



Det vigtigste aspekt ved CBDC, der adskiller det fra andre elektroniske betalingsmidler, er dets status som lovligt betalingsmiddel. Med andre ord **skal en CBDC accepteres, hvis den tilbydes som betaling inden for en jurisdiktion,** mens andre elektroniske betalingsmidler kan afvises.

Både fysiske og digitale tokens udstedes direkte af centralbanker. Dette aspekt - tilføjet til status som lovligt betalingsmiddel - er den største forskel mellem CBDC på den ene side og private penge og de næsten 22.000 forskellige kryptovalutaer (inklusive omkring 9000 af de bedste stablecoins)[4] udstedt af private aktører i de seneste år,[5] i takt med den seneste udvikling inden for distribueret ledger-teknologi (DLT) og kryptografi.

Det faktiske digitale betalingslandskab er drevet af kommercielle banker, og overførsler foretages udelukkende med private penge. Derudover har kunderne krav på at hæve deres penge i form af kontanter udelukkende til den kommercielle bank, hvor disse penge er indsat. Af denne grund er der risici forbundet med solvensen i den bank, hvor personen har indsat kontanter, og tilliden mellem indehavere og banker er et nøgleelement for hele systemets funktion.

Med CBDC vil situationen være mere lig kontanter. Faktisk vil de involverede parter i transaktionen, på grund af CBDC'ens status som lovligt betalingsmiddel, have **et direkte krav på den centralbank,** der udsteder CBDC'en, selv i scenarier, hvor transaktioner forbliver formidlet af kommercielle banker. Med andre ord vil det beløb, som en indehaver i en privat bank ejer i form af CBDC, ikke gå tabt i tilfælde af konkurs. Af denne grund er solvensrisikoen meget lav. Denne ændring i betalingsmekanismerne er af nogle forfattere blevet betragtet som en ændring i betalingssystemets "sjæl", der giver mulighed[6] for et sikrere og mere solidt finansielt system at vokse under dette perspektiv. Samtidig kræver faldet i bankindskud på grund af CBDC en begrænsning (og muligvis en tærskel pr. borger for det maksimale beløb af CBDC, som enkeltpersoner kan besidde) for at undgå mangel på indskud i banker og dermed mangel på investeringer fra banker via (reduceret) indskudt penge. Under dette synspunkt udgør CBDC risici for det finansielle system, der skal håndteres.

Samlet set er beslutningen om at udstede en CBDC ikke kun et teknisk, men også, om ikke primært, et politisk valg, som kan have en betydelig indvirkning på økonomien såvel som på borgernes rettigheder og friheder og på samfundet som helhed.

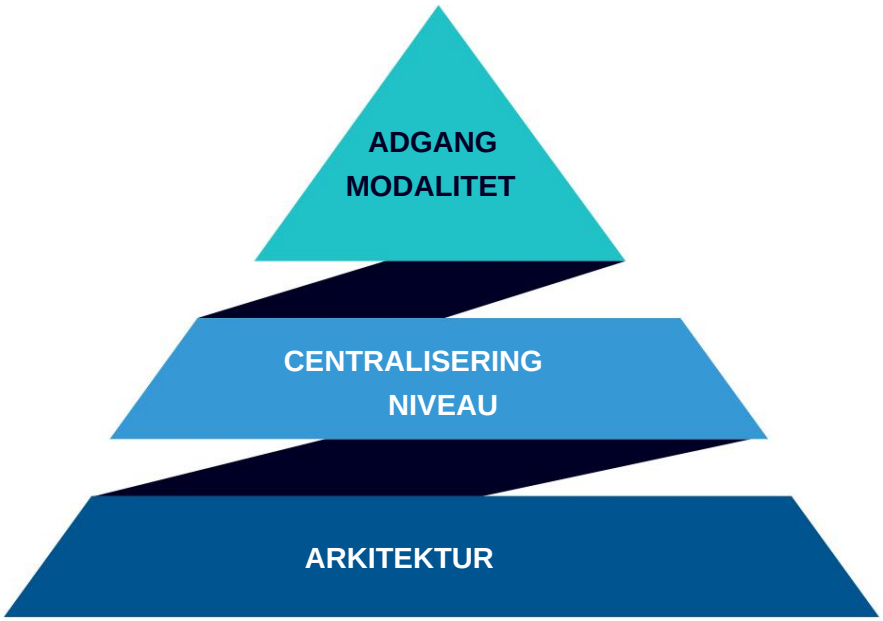
4. Kilde: **https://www.forbes.com/advisor/investing/cryptocurrency/different-types-of-cryptocurrencies/**
5. CoinMarketCap - **https://coinmarketcap.com/view/stablecoin/ (tilgået i oktober 2023).**
6. VoxEU CEPR, Centralbankens digitale valuta: kampen om det finansielle systems sjæl, 2021 - **https://cepr.org/voxeu/kolonner/centralbank-digital-valuta-kamp-sjæl-finansielt-system**

Machine Translated by Google



## 1.1 Hvad er det mulige design af CBDC?

**Design og implementering af CBDC kræver tekniske og organisatoriske valg.** De specifikke designvalg er ikke rene teknologiske elementer, men har dybtgående implikationer for det underliggende økonomiske paradigme og for mange andre politikrelaterede spørgsmål, herunder betalingers privatliv. De vigtigste designvalg vedrører: 1) den underliggende arkitektur; 2) centraliseringsniveauet; og 3) adgangsmetoden.



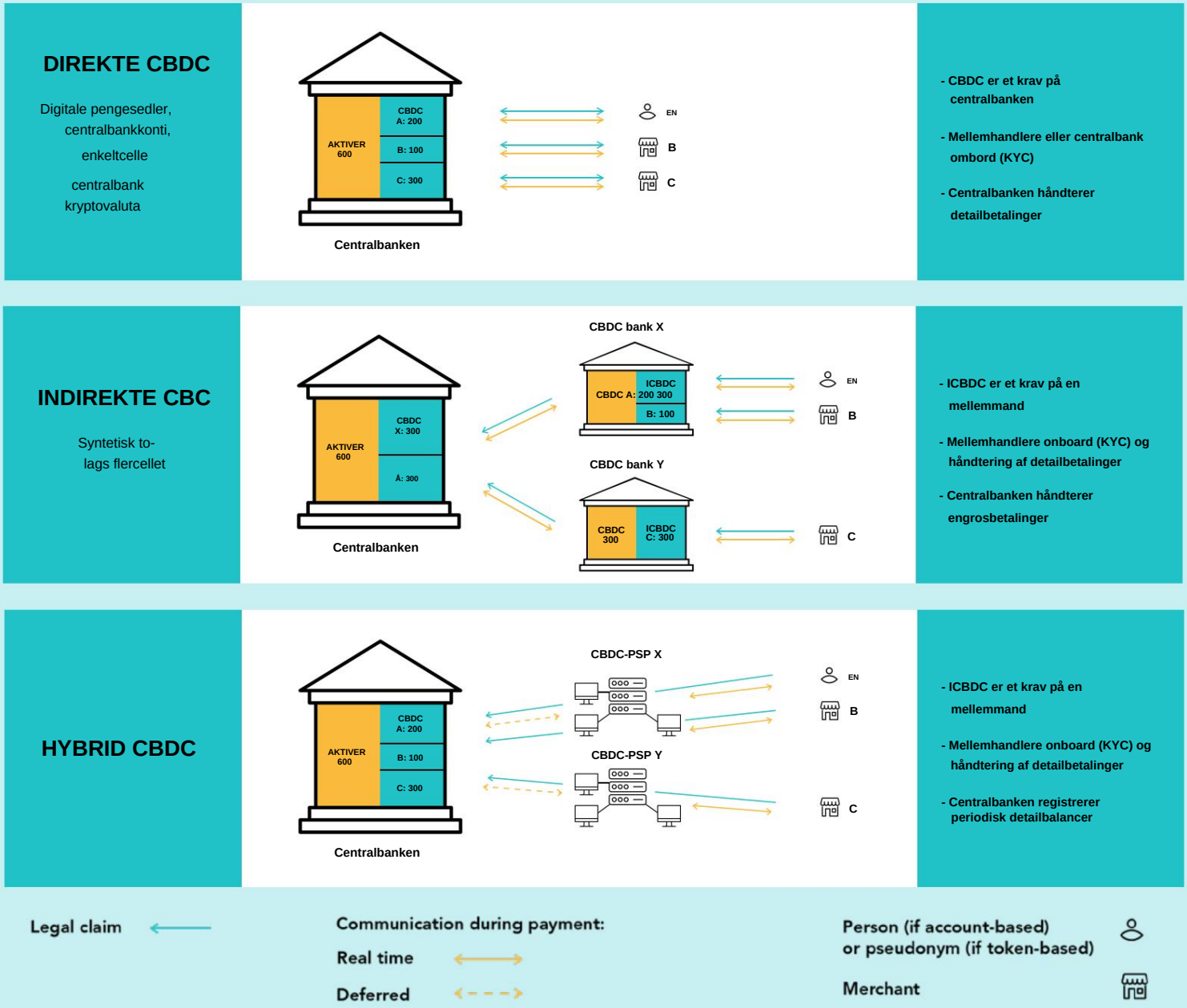

Figur 1 - Forskellige lag af designvalg, der skal træffes i processen med at implementere en CBDC

1) **Arkitekturen** relaterer sig til centralbankens og private institutioners operationelle roller i transaktionsstyring. En direkte, indirekte eller hybrid tilgang overvejes. En **indirekte** CBDC minder meget om det faktiske betalingssystem, hvor kommercielle banker administrerer transaktioner bakket op af centralbankpenge. I dette tilfælde fører centralbanken ingen registrering af transaktioner, og enkeltpersoner har kun krav mod kommercielle banker. I stedet administreres konti i en **direkte** CBDC-arkitektur direkte af centralbanken, som er den eneste institution, der håndterer betalinger. Dette scenarie er et fundamentalt skift fra dagens betalingssystem og kan medføre en dramatisk stigning i centralbankens operationer. Endelig kan **hybridmodeller** overvejes. Her opbevarer enkeltpersoner penge i centralbanken, men betalingskæden forvaltes fortsat af kommercielle banker. Nogle af de mulige fordele ved denne løsning omfatter lettere overførsel af en CBDC-konto fra en kommerciel bank til en anden, hvilket reducerer virkningerne af tekniske fejl eller konku

Machine Translated by Google



Figur 2 - Datastrømme i den forskelligartede konfiguration af arkitekturen i en CBDC




2) **Centraliseringsniveauet** for CBDC-transaktionsstyring er et andet vigtigt designvalg. CBDC'en kan være baseret på en konventionel centralt styret database eller en ny DLT. Begge teknologier lagrer ofte data på fysisk separate steder. Hovedforskellen ligger i, hvordan data opdateres. I konventionelle databaser lagres data over en eller flere fysiske noder under kontrol af én autoritativ enhed, normalt den kontrollerende bank, der validerer transaktioner. I DLT-løsninger administreres ledger'en i fællesskab af forskellige enheder på en decentraliseret måde og uden en enkelt autoritativ enhed. Blockchain er en mulig distribueret ledger-teknologi, hvor nye poster først samles i "blokke" og derefter sekventielt forbindes med hinanden og danner en kæde. Fordi hver blok indeholder et kryptografisk kodet resumé af den foregående, er blockchain'en svær at manipulere med.

[7]

,

7. For mere information om blockchain-teknologier, se **https://www.oreilly.com/library/view/masteringbitcoin/9781491902639/ch07.html**

Machine Translated by Google



Derfor skal hver opdatering af ledgeren harmoniseres mellem alle enheders noder. Den deraf følgende reducerede driftshastighed kan begrænse direkte CBDC til små jurisdiktioner. På den anden side kan DLT'er lettere anvendes i indirekte CBDC-arkitektur, da antallet af transaktioner, der skal håndteres af centralbanken, er begrænset, da de fleste af de samlede betalinger vil blive håndteret af kommercielle banker.

3) **Adgangsmetode** vedrører hvordan og til hvem bankerne skal give adgang til tokens til slutbrugere ("borgere"). En første mulighed er at følge den konventionelle **bankkontomodel** og knytte ejerskabet til en dokumenteret identitet. En "bærerbaseret", også kaldet **"tokenbaseret",** mulighed er også en mulig adgangsmetode. Her skal indehaveren demonstrere kendskab til bestemte oplysninger, såsom en privat nøgle (eller digital signatur).

Et vigtigt aspekt forbundet med adgangsmetoden er også den offline-brugervenlighed af en CBDC. Mens onlinetransaktioner kan foretages via websteder og apps, kan offlinebetalinger foretages via smartkort, mobile enheder og betalingsterminaler, der er forudfinansieret med et antal digitale tokens, der trækkes fra den saldo, som en bruger har online (på sin bankkonto), før de bruges offline. Den betroede enhed ville indeholde den aktuelle saldo og justere den ved betaling fra brugeren foretaget via kontakt eller kontaktløse metoder (f.eks. NFC-funktioner eller Bluetooth). Offlinefunktionalitet (med peer-to-peer-validering[8] af transaktioner) undgår deling af transaktionsoplysninger med andre parter end betaler og betalingsmodtager, hvilket gør det muligt for CBDC'en at blive en ækvivalent til kontanter.

Programmerbarhed[9] af CBDC er også et vigtigt designvalg. **Programmerbare betalinger** er forskellige fra **programmerbare penge.** Programmerbare penge består af en CBDC med indbyggede regler, der pålægger begrænsninger på brugen af disse penge. Med denne funktion kan en regering også definere en positiv eller negativ rente for at incitamentere eller afskrække brugen af penge til køb af en bestemt vare; begrænse deres brug til en bestemt kategori af tjenester; fastsætte en udløbsdato.

**Programmerbare betalinger** muliggør automatiske pengeoverførsler, når forudbestemte betingelser er opfyldt. For eksempel kan en person instruere sin bankkonto til at sende et bestemt beløb til en anden konto ved udgangen af hver måned. I et maskine-til-maskine-betalingsscenarie kan betalinger automatiseres, og penge kan sendes, når en pakke kontrolleres som leveret i et bestemt lagerlokale. Samtidig kan CBDC bruges som betalinger, der er programmeret som automatiske overførsler af en statslig aktør (f.eks. til velfærdsydelser).
Mens **programmerbarhed af penge** skal være integreret i de centrale designfunktioner i en CBDC, og det er noget, der sjældent er blevet implementeret nativt i det nuværende betalingssystem, er sagen for **programmerbare betalinger** anderledes.

8. For mere information om NFC-protokollen, se Wikipedia - **https://en.wikipedia.org/wiki/Near-field_communication** (tilgået i oktober 2022).
9. For mere information om programmerbare penge, se Federal Reserve, FED Notes, What is programmeable money?, juni 2021, tilgængelig på **https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.html**

Machine Translated by Google



Vi kan allerede programmere vores betalinger via bankkonti. På samme måde vil programmerbarheden af penge i tilfælde af CBDC blive leveret som værdiskabende tjenester af finansielle institutioner til deres kunder (især virksomheder og borgere) oven i CBDC-infrastrukturen.[10]

De forskellige designvalg, der er beskrevet indtil videre, kan resultere i meget forskellige brugeroplevelser. For eksempel, i tilfælde af en decentraliseret, indirekte, kontobaseret løsning, vil brugerne muligvis ikke opleve større ændringer i brugeroplevelsen i forhold til de faktiske betalingsmidler (med undtagelse af det mulige loft pr. bruger).

I det modsatte scenarie med en **centraliseret, direkte, tokenbaseret løsning** vil brugerne stå over for en større ændring i betalingsoplevelsen, da de bliver nødt til at differentiere deres udgifter mellem en CBDC-wallet og de klassiske betalingsinstrumenter, der tilbydes af kommercielle banker.

## 1.2 Hvorfor udstede en CBDC?

Teknologiske løsninger og designvalg udløses af den primære begrundelse for udvikling af CBDC'er, der forfølges på politisk niveau. Styrkelse af monetær suverænitet, strategisk autonomi og implementering af pengepolitik er de mest relevante. Udviklingen af CBDC'er kan også ses som et svar på den bredere tendens til skabelse af nye former for privat penge af private aktører, der omgår de eksisterende bankbaserede betalingssystemer.

Derudover kan CBDC'er designes med andre vigtige funktioner. Først og fremmest[11] at stimulere konkurrence og innovation inden for betalinger, fjerne barrierer og undgå lukkede betalingssystemer skabt af platforme (f.eks. Metas forsøg på at implementere sin kryptotoken kaldet "Diem"). For det andet at fremme finansiel inklusion, hvilket gør processen lettere for folk, der i øjeblikket ikke har en bankkonto. For det tredje at forbedre grænseoverskridende detailbetalinger.
Selvom Den Europæiske Union reducerer barrierer, er indenlandske betalingssystemer ofte ikke[12] interoperable mellem lande over hele verden. Den nuværende systemarkitektur har en tendens til at være langsom, dyr og vanskelig at automatisere. Derudover er risiciene forbundet med hvidvaskning af penge, skatteunddragelse og terrorfinansiering typisk høje, mens CBDC-funktionerne i forbindelse med identificerbarhed af slutbrugeren og sporbarhed af deres transaktioner kan gøre dette værktøj mere effektivt til at forhindre hvidvaskning af penge/finansiering samt svig.

10. For mere information om programmerbarhed af penge og betalinger, se PG Sandner, The Digital Programmable Euro, Libra and CBDC: Implications for European Banks, Konference: EBA Policy Research Workshop: Nye teknologier i banksektoren – virkninger, risici og muligheder, 2020.
11. Bank for International Settlements, BIS Papers No 125, Får momentum – Resultater af BIS-undersøgelsen om centralbanker i 2021 digitale valutaer, af Anneke Kosse og Ilaria Mattei, maj 2022
12. For yderligere oplysninger om Den Europæiske Unions arbejde med grænseoverskridende betalinger inden for EU, se Europa-Kommissionen, Ofte stillede spørgsmål: Grænseoverskridende betalinger inden for EU, februar 2019, tilgængelig på **https://ec.europa.eu/kommission/pressehjørne/detalje/sv/MEMO_19_1170**

Machine Translated by Google



Grænseoverskridende CBDC'er, hvor et eller flere systemer automatisk håndterer grænseoverskridende betalinger mellem flere indenlandske CBDC'er, kan forbedre grænseoverskridende betalinger betydeligt. finansielle transaktioner.[13]

Endelig er et yderligere argument for centralbankpenge, at de er af bedre kvalitet end andre former for penge skabt af kommercielle banker, fordi de ikke er afhængige af en privat udsteders solvens. Dette kan dog have en dybtgående negativ indvirkning på det nuværende banksystem. Faktisk kan tilgængeligheden af sådanne sikre aktiver tilskynde sparere til at hæve deres bankindskud og flytte pengene til deres digitale valuta-pung eller konti i centralbanken, hvilket forårsager en betydelig forstyrrelse af likviditeten i kommercielle banker.

Af disse grunde, som fremhævet ovenfor, kan centralbanken, der udsteder CBDC'en, pålægge grænser i form af lofter/lofter for kontohavere, hvor kun en begrænset mængde digital valuta kan ejes af hver person.

Med en "tiering-tilgang" findes der i øvrigt ingen hård grænse, men beholdninger over en vis tærskel vil blive afskrækket af gebyrer eller negativ rente. Den hårde grænse kan sameksistere med "tieringen" (dvs. penge over en vis tærskel vil modtage en negativ rente, og der vil dog være en maksimal tærskel for alle CBDC'er, inklusive den med negativ rente). Samtidig er der blevet udtrykt tvivl om merværdien af CBDC'er sammenlignet med eksisterende detailløsninger til betalinger.[14]

Afslutningsvis er en CBDC et politisk projekt baseret på komplekse tekniske og organisatoriske designvalg, der er strengt forbundet med de politiske mål, som centralbankerne forfølger. statslige aktører. Uanset de specifikke politiske mål, der forfølges via CBDC-projektet, er det under alle omstændigheder nødvendigt at vedtage en kompleks og robust lovgivningsmæssig ramme for at håndtere mange udfordringer, herunder privatlivs- og databeskyttelse.

13. Behovet for formidlere ville blive reduceret eller elimineret ved at give banker mulighed for direkte at opbevare udenlandske CBDC'er; og korrespondentbankvirksomhed ville blive fremskyndet gennem automatiserede eller integrerede compliance- og gyldighedskontroller på en interoperabel digital platform; begge dele fører til reduceret latenstid og gebyrer for slutbrugerne. - **https://www.atlanticcouncil.org/wp-indhold/uploads/2022/09/Privatliv_i_grænseoverskridende_digital_valuta-_En_transatlantisk_tilgang__-.pdf**

14. Se blandt andet Nationalbankens analyse, Nye typer digitale penge, 23. juni 2002, side 28: "På nuværende tidspunkt, og med de tilhørende omkostninger og mulige risici, er det ikke klart, hvordan detail-CBDC'er vil skabe en betydelig merværdi i forhold til de eksisterende løsninger i Danmark." Undersøgelsen er tilgængelig på: **https://www.nationalbanken.dk/en/publikationer/Dokumenter/2022/06/ANALYSE_nr._Nye%20typer%20af%20digitale%20penge.pdf**

Machine Translated by Google



# 2. Hvad er privatlivs- og problemer med databeskyttelse?

Afhængigt af de tekniske designvalg , der træffes for en CBDC, kan der opstå forskellige udfordringer inden for privatlivets fred og databeskyttelse. En **nylig undersøgelse foretaget af Den Europæiske Centralbank (ECB)** viste, at privatlivets fred er blandt de mest presserende problemstillinger for europæiske borgere. Hvis det implementeres uden ordentlige sikkerhedsprotokoller og en tilstrækkelig arkitektur, kan privatlivets fred og sikkerhedsproblemer i forbindelse med en CBDC have en stor indvirkning på grund af omfanget af sådanne projekter. Meget vil også afhænge af de politiske mål og anvendelsesscenarier for CBDC'en. Det er derfor nøglen at integrere databeskyttelses- og privatlivskrav i kernekonceptet for en CBDC og at opretholde en konsekvensanalyse af databeskyttelse over tid for at kunne træffe de nødvendige foranstaltninger. Samtidig er en klar specifikation af de politiske mål og anvendelsesscenarier samt det mulige samspil med andre aspekter og digitale politiske initiativer afgørende.

## 2.1 Spørgsmål vedrørende privatliv og databeskyttelse i betalinger kan forværres ved bestemte designvalg

Designvalg har stor indflydelse på, hvordan privatlivets fred sikres, administreres og bevares.
På den ene side kan en **kontobaseret** CBDC-løsning kræve verificerede identiteter for alle kontohavere for at **knytte hver enkelt person til én identifikator på tværs af hele betalingssystemet.** af både funktionsmæssige og sikkerheds-/overholdelsesmæssige årsager, hvilket repræsenterer udfordringer med hensyn til privatliv og databeskyttelse. På den anden side, selvom en **tokenbaseret** tilgang i princippet kan tilbyde en mere universel adgang og bedre databeskyttelse, er der ulemper såsom risikoen for at tabe penge, hvis slutbrugerne ikke opbevarer deres nøgle sikkert.

Derudover kan visse designvalg i den underliggende teknologiske infrastruktur forværre de privatlivs- og databeskyttelsesproblemer, der allerede findes i det nuværende digitale betalingslandskab. For eksempel kan ulovlig brug af transaktionsdata til kreditvurdering og misbrug af markedsføringsinitiativer blive endnu lettere afhængigt af det niveau af datatilgængelighed, der er aftalt for hver aktør i betalingsprocessen (og som muliggøres af den enkelte og vedvarende CBDC-brugeridentifikator, som mulighed for brugerprofilering).

De teknologiske valg i et nyt CBDC-projekt kan potentielt påvirke alle borgere, der bor i en centralbanks jurisdiktion, hvilket resulterer i omfattende behandlingsaktiviteter med høje risici for de registreredes rettigheder og friheder.

Machine Translated by Google



Af denne grund bør krav til privatlivs- og databeskyttelse integreres i de lovgivningsmæssige rammer og i de centrale teknologiske beslutninger om projektets design, og alle beslutninger vedrørende funktioner, konfigurationer og risikoaccept bør evalueres og dokumenteres behørigt. En konsekvensanalyse af databeskyttelse skal udføres og vedligeholdes over tid og på tværs af forskellige faser af CBDC-projektet. Fra begyndelsen bør CBDC-designforsknings- og udviklingsprocessen opbygges med en klar tilgang til databeskyttelse by design og databeskyttelse by standard.[15] Hvis det nogensinde er muligt, vil eftermontering af en CBDC på grund af et forkert designvalg, ud over de økonomiske omkostninger, resultere i højere direkte og indirekte omkostninger og yderligere usikkerheder, der kan føre til, at borgere og virksomheder ikke længere accepterer selve projektet.

Der vil opstå kompleksiteter, hvis distribuerede ledger-teknologier er involveret i udviklingen af en CBDC, især hvad angår principper for dataminimering og lagringsbegrænsning på grund af en blockchains tilføjelsesbaserede og stadigt voksende karakter.[2]
Derudover indebærer udformningen af en CBDC risici for privatlivets fred og databeskyttelse med hensyn til grænseoverskridende betalinger.[3] Betalingsoperationer skal overholde nationale regler, og på trods af internationale standarder kan der være betydelige forskelle i implementeringen og kontroversielle grænseoverskridende samspil. Dette vil sandsynligvis yderligere komplicere implementeringen og designet af grænseoverskridende CBDC'er på grund af uforeneligheder, herunder mellem regler for privatlivets fred, databeskyttelse og bekæmpelse af hvidvaskning af penge (AML).

Disse potentielle problemer kan afhjælpes gennem korrekt design samt multilateral koordinering for at tilpasse tekniske, regulatoriske og tilsynsmæssige rammer. Standardiserings- og harmoniseringsindsatser, der omsættes til ensartede standarder for privatliv og gennemsigtighed, kan også implementeres for at sikre interoperabilitet på tværs af jurisdiktioner og over tid.[16]

## 2.2 Risici ved privatlivets fred i forbindelse med betalinger at blive formindsket

I dag er **kontanter** den eneste form for penge, der udveksles **anonymt** – under visse grænser – og som opererer inden for regulerede områder.[17] På grund af den øgede anvendelse af digitale betalingsmidler og reduceret brug af kontanter som betalingsmiddel kan kontanter blive marginaliseret om få år.[18] Faktisk kan anonymitet sikres for kontantbetalinger, som kan udveksles mellem to ligestillede uden en tredjepart, der validerer transaktionen.

15. For en mere omfattende forklaring af konsekvensanalyse vedrørende databeskyttelse i EU, se artikel 29 i Databeskyttelsesgruppen, Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandling "sandsynligvis vil resultere i en høj risiko" i henhold til forordning 2016/679, senest revideret og vedtaget den 4. oktober 2017.
16. For mere information om privatlivsproblemer i forbindelse med grænseoverskridende betalinger, se Atlantic Council - Geoeconomics Center, Privacy in Cross-border Digital Currency - A Transatlantic Approach, 2022 - tilgængelig på **https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privatliv_i_grænseoverskridende_digital_valuta-_En_transatlantisk_tilgang__-.pdf**
17. Forskellig sektorlovgivning har allerede afvejet betalingsmodtageres privatliv mod andre konkurrerende værdier. Faktisk forbyder direktivet om bekæmpelse af hvidvaskning af penge kredit- og finansieringsinstitutter at føre anonyme konti eller anonyme bankbøger, og det definerer også tærskler for beløb, hvor due diligence-processer skal anvendes. For yderligere information, se direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvaskning af penge eller finansiering af terrorisme.
18. For yderligere information, se Den Europæiske Centralbank - Undersøgelse af forbrugernes betalingsadfærd i euroområdet (SPACE) – 2022.

Machine Translated by Google



På den anden side muliggør de private digitale betalingsløsninger, der er tilgængelige på markedet, en stigende dataudnyttelse, hvilket fører til en reduktion af anonyme betalinger. **Anonymitet under en vis tærskel kan blive et klart unikt træk ved den tokenbaserede CBDC-løsning** (som er et ihændehaverinstrument ligesom pengesedler), hvilket **adskiller den fra alle andre private digitale betalingsmetoder, der anvendes af borgerne.** Dette ville være en unik mulighed for borgerne, da sikre, stabile og anonyme kontantløse betalinger ikke eksisterer i øjeblikket.

**Offline-løsninger** (f.eks. den tokenbaserede CBDC, der ville have offline-transaktionskapacitet) kan potentielt tilbyde det bedste med hensyn til privatliv og databeskyttelse, da kun minimale behandlingsoperationer er nødvendige for at gennemføre transaktionen.

Derudover behandles offlinebetalinger lokalt uden behov for tredjepart til at validere transaktionen. Offlinebetalinger er også en sikker backup i tilfælde af større internetafbrydelser. Den tokenbaserede CBDC, der ville have offline-transaktionsfunktion, kunne funktionelt set svare til kontanter eller en godkendt check.

På grund af CBDC's digitale natur er det i sagens natur mere gennemsigtigt. Fuldt anonyme CBDC-løsninger kan være vanskelige at forene med behovet for at forhindre ulovlige aktiviteter såsom narkotikahandel, hvidvaskning af penge og finansiering af terrorisme, der er afhængige af anonyme kontanttransaktioner eller alternative pengeoverførselssystemer. Her kan lovgiveren definere den korrekte balance og de nødvendige anvendelsesscenarier, som kan implementeres gennem avancerede pseudonymiseringsteknikker blandet med andre privatlivsfremmende teknologier.[19]

Endelig skal der defineres en passende løsning til identifikation og tilladelse af adgang til og brug af offline digitale tokens. **Kontobaseret** identifikation kan føre til identifikation og potentiel sporing af alle slutbrugeres transaktioner og profilering heraf (se afsnit 2.5), mens et offline tokenbaseret CBDC-system ville muliggøre anonyme betalinger.

19. For yderligere information, se World Economic Forum, The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value, september 2019 og Future of Financial Intelligence Sharing (FFIS), Innovation and discussion paper: case studies of use of privacy preserving analysis to tackle financial crime, januar 2021.

Machine Translated by Google



## 2.3 Den resulterende interferens af adoptionen og brugen af CBDC på folks privatliv opfylder muligvis ikke nødvendighedens krav og proportionalitet

Ethvert designvalg, der resulterer i en indblanding i folks privatliv, skal bevises at være nødvendigt for det sociale behov eller den politiske målsætning, som CBDC-projektet forfølger. Derudover skal hver designmulighed overvejes under nødvendigheds- og proportionalitetsprincippet for at afgøre, om alternative teknologier og processer kan levere sikrere løsninger.

Især kan der opstå risici for enkeltpersoner, når privatliv og databeskyttelse skal afvejes med andre værdier og rettigheder, der skal beskyttes. Ligesom alle andre betalingsmidler skal CBDC'er udvikles i overensstemmelse med andre gældende love og regler i en sektor, der er en af de mest regulerede i databehandlingslandskabet.

For eksempel, ligesom det er tilfældet for ikke-CBDC-brug, kræver lovgivning om bekæmpelse af hvidvaskning af penge, finansiering af terrorisme og skatteunddragelse specifik behandling af personoplysninger. Det særlige design og de særlige funktioner ved en CBDC kan resultere i en specifik risikoprofil i forbindelse med bekæmpelse af hvidvaskning af penge og finansiering af terrorisme, der er forskellig fra den, der findes for andre betalingsmidler og kontanter. Derfor bør disse aspekter også behandles fremadrettet inden lanceringen af et CBDC-projekt.[20]

Derudover skal indvirkningen på privatlivets fred vurderes omhyggeligt for at finde den rette balance med specifikke og konkurrerende interesser i CBDC, såsom brugervenlighed og revisionsvenlighed. Afhængigt af den valgte tekniske løsning, for eksempel en fuldt centraliseret CBDC med klar og vedvarende brugeridentifikation og fuld gennemsigtighed i alle en brugers onlinetransaktioner, kan der opstå risiko for generaliseret overvågning (se afsnit 2.5).

20. Finansiel Aktionsgruppe (FATF), Opdateret vejledning til en risikobaseret tilgang, Virtuelle aktiver og virtuelle aktivtjenester udbydere, 2021

Machine Translated by Google



## 2.4 Roller og ansvarsområder er komplekse at identificere

I henhold til de specifikke designvalg, som centralbanken har vedtaget, kan forskellige aktører inden for betalingsøkosystemet behandle personoplysninger (se figur 2). Anerkendelse af databeskyttelsesroller er af allerstørste betydning for en korrekt anvendelse af forpligtelser og ansvar i henhold til gældende databeskyttelseslovgivning. Den decentraliserede forvaltning og de mange aktører, der er involveret i behandlingen af data, kan føre til vanskeligheder, hvis en DLT-baseret arkitektur implementeres. Omend vanskeligt, er identifikationen af den/de dataansvarlige det første element, der er nødvendigt for at fordele databeskyttelsesansvaret på tværs af betalingskæden.

For eksempel er **forholdet mellem centralbanker og de finansielle formidlere** afgørende for at afgøre, hvem der skal anmelde et muligt brud på persondatasikkerheden, eller hvem de registrerede skal kontakte for at udøve deres ret til information, adgang eller til at trække deres tilladelse tilbage.
samtykke.

## 2.5 Systemiske risici ved profilering og overvågning er til stede

Som allerede rapporteret i vores **TechDispatch #2/2021 om kortbaserede betalinger,** Sporing af en persons betalinger kan beskrive forbrugernes liv i detaljer og dermed forstå folks online- og offline-forbrugsvaner. Mængden af personlige oplysninger, som aktører involveret i transaktionsstyring får kendskab til om hver enkelt person, når et betalingssystem fungerer, er betydelig. Dette skaber en systemisk risiko for profilering og overvågning foretaget af de parter, der driver betalingssystemet. Specifikt inden for CBDC-domænet er denne risiko forbundet med designvalg. For eksempel kan et design, der ikke tillader centralbanker at behandle personoplysninger, eller som implementerer streng dataminimering, undgå eller reducere de risici for privatlivets fred, der er forbundet med de nuværende betalingssystemer.

Tværtimod kan en konfiguration, der tillader centralbanken at identificere og lagre personlige oplysninger om betalingerne, eller hvor forhandlere kan indsamle og forbinde betalingsdata med kundeprofiler, forstærke disse risici sammenlignet med de nuværende betalingsmetoder.[21]

21. En forhandler repræsenterer en person eller virksomhed, der sælger varer eller tjenester – for mere information, se venligst Stax Payments, Explained Simply: What is a Merchant Services Provider?, tilgængelig på **https://staxpayments.com/blog/merchant-services-provider/**

Machine Translated by Google



Derudover øger udstedelsen af en CBDC centralbankens – og dermed andre offentlige myndigheders – mulighed for at få adgang til finansielle oplysninger, der er direkte knyttet til en identitet, hvilket indebærer risiko for systemisk offentlig overvågning. Uanset om den genanvendes i fremtiden, overføres til en anden offentlig myndighed eller lækkes ved et uheld, udgør en så enorm datasamling en generel risiko for masseovervågning og utilsigtet brug.

Af disse grunde bør der anvendes privatlivsfremmende teknologier, herunder avancerede pseudonymiseringsteknikker og nul-viden-sikring, for at begrænse oplysninger, der deles mellem transaktionspartnere, til det minimum, der er nødvendigt for at bevise, at betalingen er gennemført.

Derudover er det et centralt krav at definere og pålægge specifikke opbevaringsperioder for personoplysninger i forbindelse med hvert formål med databehandlingen, også for at reducere risici i tilfælde af databrud eller ulovlig adgang til CBDC's teknologiske infrastruktur.

## 2.6 Datakoncentrationen kan øges sikkerhedsrisici

Indtil for nylig er der blevet udført meget lidt offentligt arbejde inden for cybersikkerhed og centralbankverdenen for reelt at forstå de risici, der er specifikke for CBDC.[22] Ligesom andre betalingsmidler er **sikkerhed** en nøglekomponent i en CBDC. Sikkerhed er også nøglen til at opbygge den nødvendige tillid, som borgerne skal have for at føle sig trygge ved at indføre og bruge CBDC. Adgangsoplysninger er nødvendige for at få adgang til og overføre penge. Den største risiko, tyveri eller tab af legitimationsoplysninger, er fælles for de fleste andre betalingsmidler. Faktisk kan tyveri og tab af legitimationsoplysninger resultere i kompromittering af konti og data. Moderne angrebsteknikker såsom social engineering, sidekanalangreb og malware kan bruges til at udtrække legitimationsoplysninger fra en CBDC-brugers enhed. Virkningen af et sådant angreb kan være forstyrrende, med en vis afbødning, hvis arkitekturen implementeres til at behandle lave mængder digital data. valuta.

'Datakoncentration' er også en vigtig sikkerhedsrisiko at overveje. Faktisk ville det, hvis alle borgeres betalingsdata blev **koncentreret i en centralbanks database,** skabe incitamenter til cyberangreb og en høj systemisk risiko for individuel eller generel overvågning i tilfælde af databrud eller mere generelt ulovlig adgang, samt for denial-of-service-angreb, der bringer muligheden for at udføre betalinger i fare, især i tilfælde af "direkte" tilgang.

22. For yderligere information, se Atlantic Council, Missing key: the challenge of cybersecurity and central bank digital currency, juni 2022 - tilgængelig på **https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/**

Machine Translated by Google



På den anden side, hvor en distribueret ledger-teknologi anvendes (og datalagring finder sted på enheden), skal "double-spending"-angreb[23] minimeres tilstrækkeligt, især i den **offline, bearer-baserede** konfiguration af en CBDC. Disse består i en form for forfalskning, hvor CBDC'en bruges flere gange ulovligt.

**Kvanteberegninger** kan i sidste ende påvirke alle finansielle tjenester, da det kan kompromittere vigtige datakrypteringsmetoder og kryptografiske primitiver, der anvendes til at beskytte adgang, fortrolighed og integritet af data, der lagres og transmitteres, og behovet for mulig post-kvantekryptografi bør tages i betragtning under teknologidesign.[24]

Endelig vil fragmenterede bestræbelser på at opbygge CBDC'er på nationalt plan sandsynligvis resultere i cybersikkerhedsrisici som følge af vanskeligheder med at sikre interoperabilitet, især i en grænseoverskridende dimension. Centralbanker har hidtil fokuseret på indenlandsk anvendelse af CBDC med for lidt tankegang til grænseoverskridende regulering, interoperabilitet og standardisering. Overførsel af personoplysninger og transaktionsoplysninger på tværs af jurisdiktioner kan øge omfanget, omfanget og hastigheden af databrud.

For at kunne håndtere sikkerhedsrisici korrekt bør teknisk styring være en integreret del af et CBDC-system for at overvåge nye udviklinger og forudse risici. Indførelse af open source-modeller kan bidrage til at fremme gennemsigtighed, innovation og tillid. Sikkerhedsproblemer i CBDC-infrastrukturen, hvis relevante krav og forventninger er høje, kan få alvorlige konsekvenser blandt interessenter og et betydeligt tab af tillid fra brugerne, med deraf følgende afvisning som et udbredt betalingsmiddel, hvilket resulterer i projektets fiasko.

23. Sveriges Riksbank, Om muligheden for en kontantlignende CBDC, februar 2021 - **https://www.riksbank.se/globalassets/media/rapportør/medarbejdermemo/engelska/2021/om-muligheden-for-en-kontant-lignende-cbdc.pdf**
24. Mange banker verden over udvikler og tester allerede post-kvante sikkerhedskapaciteter. Se herom Bank for International Settlements, BIS Innovation Hub annoncerer nye projekter og udvider cybersikkerheds- og grønne finanseksperimenter, juni 2022 - **https://www.bis.org/press/p220617.htm** og Finextra, Banque de France tester 'post-kvante' sikkerhedsteknologi, september 2022 - **https://www.finextra.com/newsarticle/41018/banque-de-france-tests-post-quantum-security-tech**

Machine Translated by Google



# Anbefalede læsninger

Europa-Parlamentet, Den digitale euro: politiske implikationer og perspektiver, januar 2022 - **https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)703337**

Banca d'Italia, En digital euro: et bidrag til diskussionen om tekniske designvalg, Juli 2021

R. Auer, R. Bohme, Teknologien bag digitale valutaer i detailcentralbanker, BIS Quarterly Review, marts 2020

Digital Euro Association, Forud for den digitale euro, august 2022

Raskin et. al., Digitale valutaer, decentraliserede registre og centralbankvæsenets fremtid, National Bureau of Economic Research, 2016

Institut og Fakultet for Aktuarer, Forståelse af Centralbankers Digitale Valutaer (CBDC), Marts 2019

Den Internationale Valutafond, F&D-serien, Pengerevolutionen – Krypto, CBDC'er og fremtidens finans, september 2022

Atlantic Council, Manglende nøgle: Udfordringen med cybersikkerhed og centralbankers digitale valuta, juni 2022 - tilgængelig på **https://www.atlanticcouncil.org/in-depth-research-reports/rapport/manglende-nøgle/**

Bank of International Settlement, Digitale centralbankvalutaer: systemdesign og interoperabilitet, 2021 – tilgængelig på **https://www.bis.org/publ/othp42_system_design.pdf**

Machine Translated by Google

Denne publikation er en kort rapport udarbejdet af Teknologi- og Privatlivsenheden under Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). Den har til formål at give en faktuel beskrivelse af en ny teknologi og diskutere dens mulige indvirkning på privatlivets fred og beskyttelsen af personoplysninger. Indholdet af denne publikation indebærer ikke en politisk holdning fra EDPS.

Udgaveforfattere: Stefano LEUCCI, Massimo ATTORESI, Xabier LAREO
Redaktør: Massimo ATTORESI

Alle citerede og anførte links blev sidst tilgået den 10. marts 2023.
Kontakt: **techdispatch@edps.europa.eu**

For at abonnere eller afmelde dig TechDispatch-publikationer, send venligst en mail til **techdispatch@edps.europa.eu.** Databeskyttelsesmeddelelsen er online på **EDPS' hjemmeside.**

© Den Europæiske Union, 2023. Medmindre andet er angivet, er genbrug af dette dokument tilladt under en **Creative Commons Attribution 4.0 International License (CC BY 4.0).** Det betyder, at genbrug er tilladt, forudsat at der gives passende kreditering, og eventuelle ændringer er angivet.

Til enhver brug eller gengivelse af fotos eller andet materiale, der ikke ejes af Den Europæiske Union, skal der indhentes tilladelse direkte fra indehaverne af ophavsretten.

Machine Translated by Google

**edps.europa.eu**

@EU_EDPS

EDPS

Den Europæiske Tilsynsførende for Databeskyttelse

@EDPS@social.network.europa.eu

@EDPS@tube.network.europa.eu